THE CENTRAL OF A GROUP*

BY

G. A. MILLER

§ 1. *Introduction.*

The totality of the invariant operators of any group (G) constitutes a characteristic subgroup (K) known as the central, or the cogredient subgroup of G. When G is abelian it coincides with K, and when G contains only one invariant operator, K is the identity. In these extreme cases the concept of a central does not simplify the considerations with respect to G, but in all other cases this concept is useful. It is especially useful in the study of the groups of order p^m, p being a prime, since according to a well known theorem, due to SYLOW, the order of the central of such a group cannot be less than p. It may also be used to determine whether G is the direct product of its Sylow subgroups, since a necessary and sufficient condition that G has this property is that we arrive at the identity by forming the successive quotient groups with respect to the central.†

The quotient group (I_1) with respect to K is the group of cogredient isomorphisms of G and hence I_1 cannot involve any operator besides the identity which is generated by each operator of a possible set of generators of G.‡ In particular, I_1 cannot be either cyclic or hamiltonian and hence the index of K under G must be the order of a non-cyclic group. It is easy to see that this index cannot be an arbitrary number which is the order of a non-cyclic group. For instance, it cannot be a number which is neither a square nor the order of a non-abelian group, since an abelian group of cogredient isomorphisms cannot involve a Sylow subgroup of prime order and such a number is not divisible by the squares of all its prime factors.§

As every possible dihedral group is a group of cogredient isomorphisms of a dihedral group it results that G may be so constructed that the index of K under G is an arbitrary even number with the exception of 2. This index may also be any positive integral power of p except p itself, since the abelian group of order p^m, $m > 1$, and of type $(1, 1, 1, \cdots)$ is evidently the group of cogredient isomorphisms of some group of order p^{m+2}. These elementary considerations

* Presented to the Society (Chicago) April 18, 1908.

† LOEWY, Mathematische Annalen, vol. 55 (1901), p. 69.

‡ Bulletin of the American Mathematical Society, vol. 6 (1900), p. 339.

§ DICKSON, Transactions of the American Mathematical Society, vol. 6 (1905), p. 201.

are sufficient to prove that, if n is a number > 2 which cannot be the index of K under G, then n is odd and involves only the first power of some prime, but it is not implied that a number satisfying these conditions cannot also be the index of K under G. When I_1 is the direct product of two solvable groups whose orders are relatively prime, G is also the direct product of two such groups.* In particular, when I_1 is abelian, G is the direct product of its Sylow subgroups. This is clearly a special case of the theorem mentioned at the end of the first paragraph. When I_1 is abelian, G is said to be metabelian, and a number of fundamental properties of such a G have been determined.†

The main object of the present paper is to exhibit the usefulness of the concept of a central by presenting some relations between fundamental theorems bearing on this concept and by extending several of them so as to be more directly applicable from this point of view. We shall especially consider properties of G which may be derived from those of the quotient group with respect to its central. The paper has close contact with a memoir by HÖLDER, entitled *Bildung zusammengesetzter Gruppen*,‡ but in the present paper we assume only a knowledge of the special quotient group while HÖLDER generally assumed both a knowledge of this group and also of the corresponding invariant subgroup. One of the most important results is the theorem, proved in the last section, that I_1 may be so chosen that every possible G is the direct product of I_1 and an arbitrary abelian group.

§ 2. *Properties of G which may be derived from those of its I_1.*

Suppose that I_1 contains an invariant operator (i). The operators of G which correspond to i are transformed among themselves by all the operators of G and hence each of these operators is transformed under G into itself multiplied by an operator of K. One of these operators (s) must therefore transform every operator of G into itself multiplied by some operator of K, and hence s gives rise to at least one invariant commutator whose order is equal to the order of i. The holomorphism obtained by transforming G by s may also be obtained by making G isomorphic with a subgroup of K and multiplying corresponding operators. That is, the holomorphisms obtained by transforming G by operators which correspond to invariant operators in I_1 may be obtained in the same manner as the holomorphisms of an abelian group.§

From the preceding paragraph it results that the order of G is divisible by n^3 whenever I_1 involves an invariant operator i of order n, and that such an I_1

*Transactions of the American Mathematical Society, vol. 1 (1900), p. 69.

†FITE, Transactions of the American Mathematical Society, vol. 3 (1902), p. 331.

‡Mathematische Annalen, vol. 46 (1895), pp. 321–422.

§Bulletin of the American Mathematical Society, vol. 6 (1900), p. 337.

contains operators which are independent of i and whose orders are divisible by n. In fact, if s_1 is an operator of G which s transforms into itself multiplied by an operator of K whose order is equal to that of i, then s^α $(\alpha < n)$ cannot be commutative with s_1 and hence i^α cannot be generated by i_1, i_1 being the operator of I_1 which corresponds to s_1. This includes the theorems that in the group of cogredient isomorphisms of a metabelian group the order of every operator divides that of another independent operator and is also the order of a commutator.* These results include the following theorem: *If the group of cogredient isomorphisms of G involves an invariant operator of order n, G contains an invariant commutator of order n and it also has a cyclic quotient group of this order. Moreover, the order of G is divisible by n^3 and I_1 involves two independent operators whose orders are divisible by n.*

To every Sylow subgroup of I_1 there corresponds one and only one Sylow subgroup of G having for its order a power of the same prime. This follows directly from the fact that to each operator of I_1 whose order is a power of this prime there correspond just as many operators whose orders are a power of this prime as there are such operators in K, since K is composed of invariant operators. Hence it results that if the order of I_1 is divisible by a prime p the number of Sylow subgroups of order p^m in G is exactly the same as the number of the Sylow subgroups of order p^a in I_1. If a prime divides the order of G without also dividing that of I_1 there is only one Sylow subgroup in G whose order is a power of this prime; but the identity may be regarded as the corresponding Sylow subgroup of I_1. Hence the number of Sylow subgroups of each order in G is exactly the same as the number of the subgroups of the corresponding order in I_1. This result includes the theorem that G is the direct product of its Sylow subgroups when and only when we arrive at the identity by forming the successive groups of cogredient isomorphisms of G; for, since the identity has only one Sylow subgroup of a given order, G can have only one such subgroup when the given condition is satisfied.

The necessary and sufficient condition that a subgroup of I_1 is abelian is that all the commutators of the corresponding operators of G are in K. This includes the known theorem that if all the commutators of a group are invariant it is metabelian and vice versa. If I_1 involves an abelian subgroup which does not contain a group differing from the identity that can be a group of cogredient isomorphisms, then the corresponding subgroup of G is abelian. In particular, every subgroup of G which corresponds to a cyclic subgroup of I_1 is abelian. While an invariant operator of I_1 implies an invariant commutator of G whose order is equal to the order of this operator, the converse is not true, since an invariant commutator of G merely implies an abelian subgroup of I_1 which involves two independent operators of orders equal to the order of this commutator.

*FITE, Transactions of the American Mathematical Society, vol. 3 (1902), p. 334.

From the fact that all subgroups which correspond to invariant subgroups of I_1 are invariant under G it follows that G is solvable whenever I_1 is solvable and vice versa. In particular, when all the Sylow subgroups of I_1 are cyclic those of G must be abelian and G must be solvable. We proceed to prove that such a G does not involve any invariant commutator besides the identity. If the order of I_1 is $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$, where $p_1, p_2, \cdots, p_r$ are distinct primes such that $p_1 > p_2 > \cdots > p_r$, it is known that I_1 contains only one subgroup of order $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\lambda^{\alpha_\lambda}$ $(\lambda = 1, 2, \cdots, r)$.* Since all the Sylow subgroups of G are abelian it results that if G were to involve an invariant commutator in addition to the identity such a commutator could be obtained by using operators belonging to distinct Sylow subgroups of G, since the elements of the commutator would correspond to commutative operators of I_1. This is impossible, as the order of an invariant commutator always divides the orders of the elements of the commutator. Some of these results are included in the following theorem: *When all the Sylow subgroups of I_1 are cyclic every abelian subgroup of I_1 corresponds to an abelian subgroup of G. The necessary and sufficient condition that every abelian subgroup of I_1 corresponds to an abelian subgroup of G is that the central of G involves no commutator besides the identity. If this condition is satisfied every operator of G has the same number of conjugates as the corresponding operator of I_1.* It is clear that this condition is always satisfied when the orders of I_1 and K are relatively prime.

As I_1 must be non-abelian whenever all its Sylow subgroups are cyclic, there must be some prime divisor (p_α) of its order such that the subgroup of order $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\alpha^{\alpha_\alpha}$ $(\alpha < r)$ is cyclic while the one of order $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_{\alpha+1}^{\alpha_{\alpha+1}}$ is non-cyclic. We proceed to prove that G also contains an invariant cyclic subgroup of order $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\alpha^{\alpha_\alpha}$ involving no invariant operator under G besides the identity. The subgroup of G which corresponds to the group of order $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\sigma^{\alpha_\sigma}$ in I_1 is abelian and the number of the cyclic subgroups of order p_β^m in G which correspond to the Sylow subgroup of order $p_\beta^{\alpha_\beta}$ $(\beta = 1, 2, \cdots, \alpha)$ in I_1 is a power of p_β whenever these subgroups have been so selected that m has a minimum value. The operators of G which correspond to an operator of order $p_{\alpha+1}^{\alpha_{\alpha+1}}$ in I_1 must transform some one of the given cyclic subgroups of order p_β^m into itself without being commutative with each of its operators. It is known that *if an operator which is prime to the order of a cyclic group of order p^m, p being a prime number, transforms this cyclic group into itself, either it is commutative with every operator of the cyclic group or it is non-commutative with each one of its operators besides the identity as well as with each operator of every possible quotient group of this cyclic group.*† From this theorem it follows directly that $m = \alpha_\beta$ and that there is only one subgroup among those corre-

* BURNSIDE, *Theory of groups of finite order* (1897), p. 352.

† Annals of Mathematics (new series), vol. 3 (1902), p. 180.

sponding to the cyclic subgroup of order p^m in I_1 which is invariant under the group that corresponds to a Sylow subgroup of order $p_{\alpha+1}^{\alpha_{\alpha+1}}$ in I_1. As this subgroup must also be invariant under the groups which correspond to the conjugates of this Sylow subgroup, it follows that it is a characteristic subgroup of G. In a similar manner it may be proved that G contains a characteristic subgroup of each of the orders $p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots, p_\alpha^{\alpha_\alpha}$, and as the operators of all these subgroups are commutative it involves the direct product of these characteristic subgroups. This proves the theorem: *If I_1 contains a cyclic subgroup of order $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\alpha^{\alpha_\alpha}$, then G contains a characteristic cyclic subgroup of the same order.*

In proving this theorem we made use of the facts that I_1 is non-abelian and that each of its Sylow subgroups is cyclic; but we did not employ the fact that I_1 is the entire group of cogredient isomorphisms of G. Hence we may deduce the following useful corollary: *If I_1 involves a group containing a cyclic invariant subgroup of order g with no invariant operator besides the identity under this group, then G contains a cyclic subgroup of order g.* In particular, if I_1 contains a dihedral group whose order is twice an odd number, G contains a subgroup whose order is this odd number. If I_1 is the direct product of two cyclic groups of order n the commutator subgroup of G is a cyclic group of order n contained in K. The simplest special case of this is when I_1 is of order p^2 and hence the commutator subgroup of G is composed of p invariant operators. Every subgroup of G which involves operators corresponding to every operator of I_1 is invariant under G and involves all the commutators of G.

§ 3. *Groups in which I_1 involves only two prime factors.*

Since I_1 cannot be cyclic it must be of type $(1, 1)$ when its order is p^2, and $p-1$ must be divisible by q when its order is pq. In the former case G is the direct product of its Sylow subgroups, and all these Sylow subgroups except the one of order p^m are arbitrary abelian Sylow groups. Hence it is only necessary to consider the Sylow group G' of order p^m whose central is of order p^{m-2}. It is known that G' involves exactly $p+1$ abelian subgroups of order p^{m-1} having K' in common. Moreover, K' may be an arbitrary abelian group of order p^{m-2}. We proceed to prove that two of the given $p+1$ abelian subgroups are arbitrary groups containing K' while the other $p-1$ have the same invariants as one of these two whenever these do not involve the same invariants.

Suppose that the invariants of K' are $p^{\alpha_0}, p^{\alpha_1}, \cdots, p^{\alpha_\lambda}$ where

$$\alpha_0 + \alpha_1 + \cdots + \alpha_\lambda = m - 2 > 0$$

and at least two of these exponents are zero. The invariants of any abelian group of order p^{m-1} containing K' may be obtained by increasing one and only one of these exponents by unity. Hence it results that the invariants of two of the given subgroups of order p^{m-1} in G may be obtained by increasing by unity

successively two arbitrary exponents of the invariants of K', while the invariants of the remaining $p-1$ are the same as those of that one of these two which was obtained by increasing the larger exponent if different exponents have been increased.* By increasing the exponents of two equal invariants G' may evidently be so constructed that each of its $p+1$ subgroups involving K' has the same invariants and vice versa. We may summarize these results as follows:

When I_1 is of type $(1, 1)$ G is the direct product of an abelian group whose order is prime to p and a group G' of order p^m. The commutator subgroup of G is composed of p invariant operators, and the invariant operators of G' form a subgroup K' of order p^{m-2}. When I_1 is given, K' may be an arbitrary abelian group of order p^{m-2}, $m>2$. The $p+1$ subgroups of G' which have K' in common and are of order p^{m-1} either have the same invariants, or p of them have the same invariants while the remaining one has invariants which may be obtained by increasing a smaller exponent in the invariants of K'. In each case the invariants of these subgroups of order p^{m-1} may be obtained by increasing one and only one of the exponents of the invariants of K' by unity.

It is not difficult to determine all the groups of order p^m involving a central of order p^{m-2} and hence all the groups whose I_1 is of type $(1, 1)$. Since each distinct K' leads to different G''s we may first construct all the possible K''s. The number of these is equal to the number of partitions of $m-2$ with respect to addition. Suppose that K' is of type $(\alpha_0, \alpha_1, \cdots, \alpha_\lambda)$ where we again assume that at least two of the numbers $\alpha_0, \alpha_1, \cdots, \alpha_\lambda$ are 0's. These numbers may be divided into k sets, each set being composed of all those which are equal to each other. Hence the invariants of one of the $p+1$ groups of order p^{m-1} which involve K' may be chosen in k different ways and the second of these can be chosen in $k-1$ ways so that it may have different invariants. The $p+1$ subgroups of order p^{m-1} which involve K' may therefore be chosen in $\frac{1}{2}k(k-1)+l$ ways, l being the number of the sets which involve at least two equal numbers. For each K' there are therefore $\frac{1}{2}k(k-1)+l$ classes of groups, each class being composed of those groups in which the subgroups of order p^{m-1} involving K' are of the same type. In particular, when K' is cyclic $k=2$, $l=1$; and there are therefore only two such classes, each class being composed of a single group.

It remains only to determine the number of distinct groups in each of these classes, each class being composed of all the conformal groups involving K'. This may be done by means of the commutator subgroup. The smallest number of distinct groups in a class is clearly $k-1$, the number of different invariants in K' which exceed unity. This is also the exact number when each of the two different exponents in $\alpha_0, \alpha_1, \cdots, \alpha_\lambda$ which were increased by unity to

* In the special case when $p=2$ and when the exponents which have been increased are 0 and 1 respectively this rule need not hold. This case will be excluded in what follows.

obtain the exponent for the corresponding group of order p^{m-1} is either unequal to any other or equal to 0. If only one of these is equal to another and exceeds 0, there are k such groups; and if both are equal to others greater then 0, there are $k+1$ distinct groups. Finally, when the two exponents which are increased are either equal to 0 or belong to a set of two equal exponents, there are only $k-1$ groups. When the set to which they belong contains more than two and each number exceeds 0, there are k such groups. This completes the enumeration of all the possible types of groups that may be used for G', and G is the direct product of such a G' and an arbitrary abelian group whose order is prime to p.

When I_1 is of order pq it follows from the theorems of the preceding § that G involves a characteristic subgroup P of order p corresponding to the subgroup of order p in I_1. If q^α represents the lowest order of an operator of G corresponding to an operator of order q in I_1 it follows that P and such an operator of order q^α generate a group of order pq^α involving exactly $q^{\alpha-1}$ invariant operators and having I_1 for its group of cogredient isomorphisms. Hence it is seen that *G is the direct product of an abelian group whose order is prime to q and a group of order pq^3 whenever its group of cogredient isomorphisms is of order pq*. Such a group can be constructed only when $p-1$ is divisible by q and its commutator subgroup is P.

§ 4. *Groups whose I_1 is either the icosahedral or the octohedral group.*

If I_1 is the icosahedral group, G contains operators of orders 3 and 5 corresponding respectively to operators of these orders in I_1. We can easily prove that the lowest order of an operator of G corresponding to an operator of order 2 in I_1 cannot exceed 4. Suppose that the lowest order of such an operator s is 2^α, $\alpha > 2$, and consider the subgroup of G which corresponds to a tetrahedral group in I_1. An operator of order 3 in this subgroup transforms s into three conjugates (s, s', s'') having a common square. The order of the commutator subgroup of the subgroup of G which corresponds to the group of order 4 in this tetrahedral group cannot exceed 2. Hence s and s' generate a group of order $2^{\alpha+1}$ which involves an operator of order 2 corresponding to s''. We may therefore assume that G contains three operators which satisfy the following conditions:

$$s_1^2 = t_1, \qquad s_2^5 = t, \qquad (s_1 s_2)^3 = 1, \qquad t_1^2 = 1,$$

and that t_1, t are commutative with every operator of G.

From $(s_1 s_2)^3 = 1$ it results that $s_1 s_2 s_1^{-1} = s_2^{-1} s_1 s_2^{-1}$. Hence

$$(s_2^{-1} s_1 s_2^{-1})^5 = t \qquad \text{or} \qquad (s_1 s_2^3)^5 = t^6.$$

In order to determine a limit for the order of t we consider the product of the

operators s_1, $s_2^{-4}s_1s_2^4$ which have a common square:

$$(s_2^{-4}s_1s_2^4\cdot s_1^{-1})^5=(s_2^2s_1s_2)^5t_1=t_1t^6.$$

As t_1t^6 is transformed into its inverse by s_1* and is also commutative with s_1, the order of t must divide 12. We now consider a new set of operators of G as follows:

$$s_1'=s_1t^{-3},\qquad s_2'=s_1s_2t_1t^{10},\qquad s_1's_2'=s_2t^7,\qquad (s_1's_2')^5=t^{36}=1,$$
$$(s_1')^2=t_1t^6,\qquad (s_2')^3=t_1t^6.$$

As G contains two operators differing from the identity such that the square of one is the cube of the other and their product is of order 5, G involves either the icosahedral group or G_{120}.† As these groups are invariant under G we have proved the following theorem: *A group which has the icosahedral group for its group of cogredient isomorphisms contains as a commutator subgroup either the icosahedral group or the group of order* 120 *which has a* (2, 1) *isomorphism with the icosahedral group and involves operators of order* 4. In the former case it is the direct product of the icosahedral group and some abelian group; in the latter case it is the direct product of an abelian group and a group of order $2^\alpha\cdot 60$ involving exactly 2^α invariant operators.

When I_1 is the octohedral group it follows just as in the preceding case that G contains operators of order 3 corresponding to the operators of this order in I_1, and that the operators of G which correspond to the three conjugate operators of order 2 in I_1 include operators whose order is either 2 or 4. Hence G contains two operators which satisfy the following conditions:

$$s_1^3=1,\qquad s_2^3=1,\qquad (s_1s_2)^2=t.$$

A multiple of the possible orders of t may be obtained as follows:

$$(s_1s_2\cdot s_1^2s_2^2)^2=s_1s_2s_1^2s_2^2s_1s_2s_1^2s_2^2=s_2^2s_1s_2s_1s_2^2t^2=t^3.$$

Since s_1s_2 and s_2s_1 have a common square, $s_1s_2\cdot s_1^2s_2^2$ is transformed into its inverse by s_1s_2. Hence t^3 is also transformed into its inverse by this operator and the order of t divides 6. If $s_1'=s_1t^4$ it is clear that s_1' is also of order 3 and the given conditions may be replaced by

$$s_1'^3=1,\qquad s_2^3=1,\qquad (s_1's_2)^2=t',\qquad t'^2=1.$$

If $t'=1$, s_1' and s_2 clearly generate the tetrahedral group; and if t' is of order 2 they generate the group of order 24 which involves no subgroup of order 12, since this group is defined by two operators of order 3 whose product is of order 4 when the square of this product is commutative with these operators. This

*Archiv der Mathematik und Physik, vol. 9 (1905), p. 6.

†Transactions of the American Mathematical Society, vol. 8 (1907), p. 13.

statement results from the following equations:

$$s_1^3 = 1, \quad s_2^3 = 1, \quad (s_1 s_2)^2 = t, \quad t^2 = 1; \quad ts_1 = s_1 t, \quad ts_2 = s_2 t, \quad t \neq 1.$$

In fact the following operators constitute the quaternion group:

$$1, \ t, \ s_1 s_2, \ s_2^2 s_1^2, \ s_2 s_1, \ ts_2 s_1, \ s_1 s_2^2 s_1, \ s_2^2 s_1^2 s_2 s_1.$$

The first four of these operators constitute the cyclic group and from the relation

$$s_1^2 s_2^2 \cdot s_1 s_2 \cdot s_2 s_1 = s_1^2 s_2^2 s_1 s_2^2 s_1 = s_2^2 s_1^2$$

it results that this cyclic group is transformed into itself by $s_2 s_1$ and contains $(s_2 s_1)^2 = t$. Moreover, this quaternion group is transformed into itself by s_1, since $s_1^2 s_2 s_1^2 = (s_1 s_2^2 s_1)^{-1}$. This proves the theorem: *If a group has the octohedral group for its group of cogredient isomorphisms, its commutator subgroup is either the tetrahedral group or the group of order* 24 *which involves no subgroup of order* 12.

§ 5. *Group whose I_1 is the simple group of order* 504.

When I_1 is any soluble group G contains an invariant subgroup of prime index. With respect to this subgroup we may establish a multiple isomorphism between G and an arbitrary cyclic group whose order is divisible by this prime number. Hence it results that there is always an infinite system of different groups having the same soluble I_1 such that none of these groups is the direct product of an abelian group and a non-abelian group, whenever there is one such group. Since the simple groups of orders 60 and 168 are the groups of cogredient isomorphisms of groups of orders 120 and 336 respectively which are not direct products, it results that there is also an infinite number of different groups which are not the direct products of an abelian and a non-abelian group but have one of these groups for their group of cogredient isomorphisms. In view of these facts the following theorem is of considerable interest: *Every group which has the simple group of order* 504 *for its group of cogredient isomorphisms is the direct product of an abelian group and this simple group.*

With a view to proving this theorem it will first be established that such a G contains the group of order 56 which involves 48 operators of order 7; and that every Sylow subgroup of G is abelian. From § 2 it results that G involves operators of order 7. To a subgroup of order 8 in I_1 there corresponds a Sylow subgroup of order 2^α in G having seven conjugate divisions corresponding to the seven operators of order 2 in the subgroup of order 8 in I_1. It will now be proved that each of these seven divisions involves operators of order 2. The conjugate operators in any two of these divisions must have a common square. The order of the commutator subgroup of the operators of G which correspond

to a subgroup of order 4 in I_1 cannot exceed 2. If this were of order 2 the invariant commutator of order 2 would be a commutator of the various subgroups of G which correspond to subgroups of order 4 in I_1, for all the subgroups of order 4 in I_1 are conjugate. As three such subgroups involve the same operator of order 2, and are in a Sylow subgroup of I_1, the operators of G corresponding to this common operator of order 2 would be transformed into themselves multiplied by the same operator by all the operators of G corresponding to the seven other operators of this Sylow subgroup. This is impossible since not more than one-half of the operators of a group can transform an operator into itself multiplied by an operator differing from the identity. From this it follows that every Sylow subgroup of G is abelian and that G contains operators of order 2 corresponding to operators of this order in I_1.

It is easy to see that the number of subgroups of order 8 in G corresponding to a subgroup of order 8 in I_1 is of the form 2^m, and hence at least one such subgroup is transformed into itself by an operator of order 7 in G; that is, G involves the group of order 56 which involves 48 operators of order 7 and is simply isomorphic with a subgroup of I_1. Since all the abelian subgroups of I_1 are Sylow subgroups and all the Sylow subgroups of G are abelian it results that each operator of G has exactly the same number of conjugates as the corresponding operator of I_1. In particular, G involves 63 conjugate commutators of order 2, corresponding to the commutators of this order in I_1. Every operator of I_1 is the product of two such commutators. Let s_1, s_2 be two operators of order 2 whose product is of order 7 and let s_1', s_2' be the corresponding commutators of order 2 in G. Since $(s_1' s_2')^7$ is invariant under G and is also transformed into its inverse by s_1' the order of $s_1' s_2'$ is either 7 or 14. As s_1 is transformed into s_2 by a power of $s_1 s_2$, s_1' is transformed into s_2' by a power of $s_1' s_2'$ and hence the order of $s_1' s_2'$ is 7.

There is only one operator of order 7, in the division corresponding to $s_1 s_2$ in I_1, which is transformed into its inverse by one of the given 63 conjugate commutators of G, since all the other operators of order 7 in this division are the product of $s_1' s_2'$ and an operator of order 7 which is commutative with every operator of G. From this it follows that G contains a complete set of 216 commutators of order 7 which are characterized by the fact that each of them is the product of two of the given 63 commutators of order 2 in G. In exactly the same manner it may be observed that G contains 168 operators of order 9, characterized by the fact that each of them is the product of two of these commutators of order 2. This argument proves that the product of any two non-commutative operators in this set of 63 is a commutator of G. If two of these commutators are commutative they correspond to operators of a subgroup of order 56 in I_1 and hence their product is again a commutator. Accordingly we have proved that *the product of any two of the given* 63 *commutators of order* 2 *is a commutator of* G *and that these products lead to* 504 *distinct commutators.*

To prove that these 504 commutators constitute the commutator subgroup of G, we may arrange them in two rectangular forms, writing a group of order 8 as the first row and the group of order 56 which involves this group of order 8 and a commutator of order 7 as the first seven rows, while each of the other rows begins with an operator of order 2. From the theorem stated at the end of the preceding paragraph it follows that each of these rectangles contains the given 504 commutators. It also follows from these arrangements that the product of an operator of the first row and any one of these commutators is contained in each of these rectangles. As each of the 63 commutators of order 2 can be transformed successively into the first row by operators which transform the totality of these 504 operators into itself, it has been proved that the product of any one of these 63 commutators of order 2 into one of these 504 commutators is contained in each of these rectangles. From this it follows directly that the product of any two operators in one of these rectangles is included in the rectangle and hence these 504 operators constitute the commutator subgroup of G, and G is the direct product of this subgroup and some abelian group.